

HOW IT WORKS

Fingerprint scanning

Electronic fingerprinting techniques help link criminals with the scenes of their crimes, but how reliable is the technology – and could your fingertips be used by a clever crook to elude capture? Tom Royal gets to grips with fingerprint scanning

The idea of using fingerprints for identification dates back over a century.

In 1880 Dr Henry Faulds, a former missionary who lived in Tokyo and had founded the Tokyo Institute for the Blind, published an article in the journal *Nature*. His article suggested that fingerprints left behind at the scene of a crime might be used to identify the criminal responsible. A month later Sir William Herschel, a civil servant, wrote to the journal explaining that he had used fingerprints to identify criminals in an Indian jail.

Scotland Yard initially rejected the suggestion that it could use fingerprints to identify criminals, but by 1901 it had embraced the technology. The first known conviction based on fingerprint evidence is that of Francisca Rojas, convicted of murder in Argentina in 1892.

Today forensic fingerprinting is a well-known technique. The basic method of recovering a latent fingerprint from a crime scene will be familiar to anyone who has read a crime novel or spent an evening watching Channel 5. With the rise of automated fingerprint readers, though, fingerprint analysis is moving out of the lab and on to your desk.

Methods for analysing fingerprints have been available for some time, but now they're smaller and cheaper than ever. Microsoft sells a simple USB fingerprint scanner for less than £25 and many of the more expensive notebooks we

review have one built in. This month, we explain the various ways that a computer or gadget can identify you based on your fingerprint.

TAKE IT TO THE RIDGE

The methods for comparing fingerprints electronically are similar to those used when comparing fingerprints by eye. Human fingerprints can be classified into one of four patterns: arch, loop, tented arch and whorl. Dr Henry Faulds' original system of classification used only these simple distinctions and required a set of multiple prints to identify an individual. Even with a set of all 10 fingerprints, though, this system produces a limited number of possibilities. Modern fingerprint analysis records far more information, so different fingers almost always give different profiles. The extra information specifies the location of very small fingerprint features known as minutiae.

There are four basic types of minutiae: ridge ending, where a ridge on the fingertip suddenly stops; bifurcation, where a ridge divides into two; the dot, an isolated area of ridge; and the island, where a ridge splits into two and rejoins. There are also a number of compound minutiae formed by two or more of these elements in close proximity. When examining fingerprints manually, an expert compares the location of these tiny features on the two prints being examined. If a sufficient number of minutiae

match, the two prints are judged to have come from the same person. There is no single standard for the number of minutiae that need to match before two fingerprints are said to be identical. Different law enforcement agencies in different countries, and even different states or departments within a country, work to different levels of proof. For some time the UK used a system that required 16 matching ridges based on a 1912 paper published by Alphonse Bertillon, but this was recently abandoned.

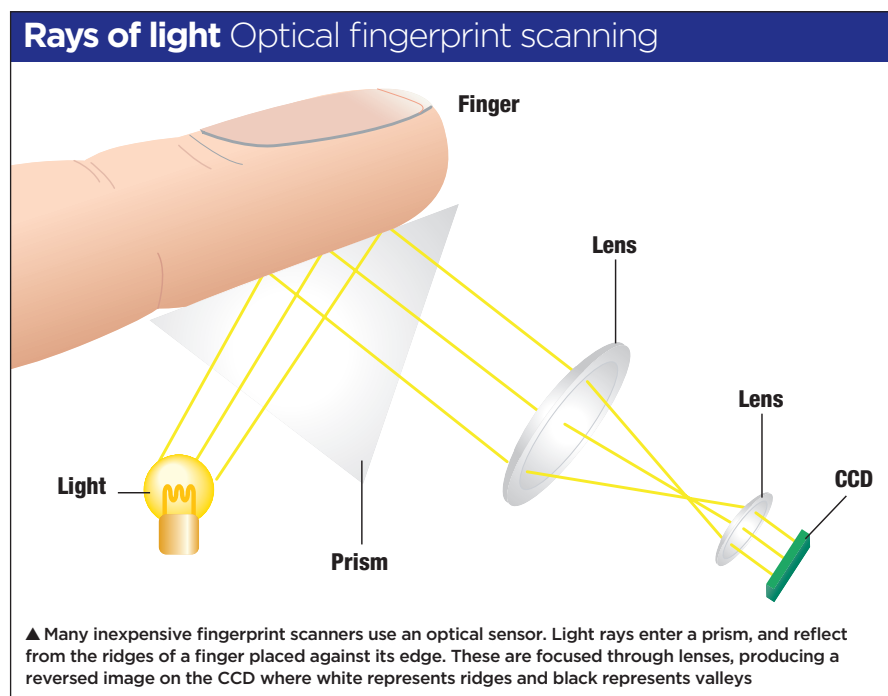
A computerised fingerprint reader also analyses each print for minutiae. Once the scanner has created a 2D image of the ridges in a subject's fingerprint, software searches for minutiae in the image. The locations are then recorded in a database. When comparing a second print to see if it comes from the same finger, its minutiae are also recorded.

An algorithm is used to compare the two sets of data and judge whether or not the two are similar enough to be considered identical. This algorithm will be run on your computer or using a microchip embedded into a device such as a fingerprint door lock. The algorithms used differ from device to device, with several companies selling algorithms to equipment manufacturers. To read the minutiae from a finger, most fingerprint scanners use one of three types of sensor: optical, capacitance or RF.

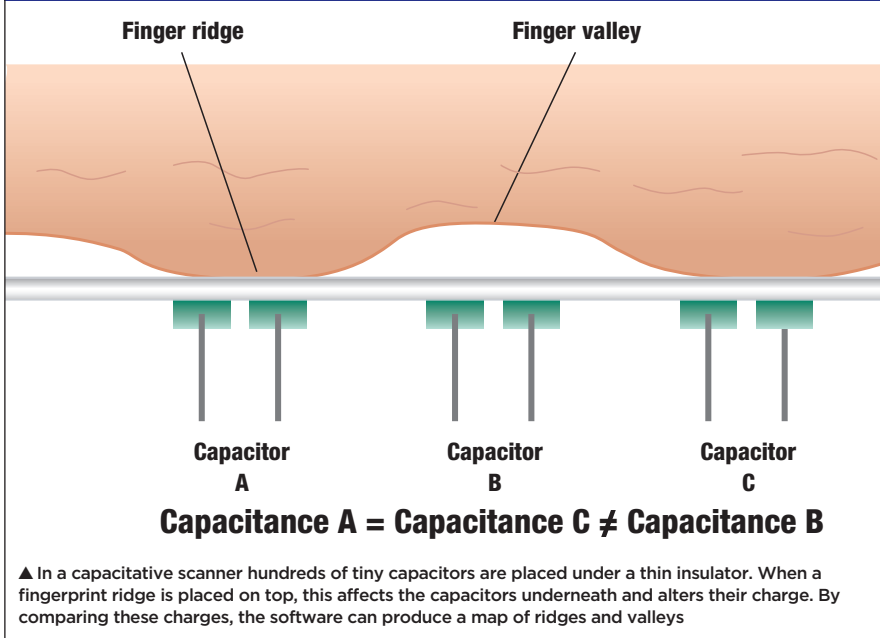
OPTIC NERVE

The simplest fingerprint scanners use an optical sensor. It's easy to imagine how such a device might work: by mounting a camera underneath a sheet of glass it should be possible to take a photograph of the fingerprint of a digit pressed on the glass. In reality, though, the process is a little more involved. Rather than a simple sheet of glass, many optical fingerprint scanners use a prism. The finger is placed against one side of this prism, and light from an LED is shone in via one of the other sides. This light hits the side of the prism with the finger. When beams hit a fingerprint ridge, they are reflected back towards the third side of the prism. Those that enter a valley in the fingerprint aren't reflected. Light emerging from the glass prism is focused by a series of lenses on to a charge-coupled device, or CCD, like those used in digital cameras. Because only ridges reflect light, the image of a fingerprint produced shows the ridges in white and the valleys dark. By inverting the image you can produce a print with ridges shown in black, just as they would be using ink and paper.

A simple optical fingerprint scanner is fairly cheap to buy – you can pick one up for less than £25 – and Microsoft even makes a keyboard with a fingerprint reader built in. These devices have



Charged Up Capacitive Fingerprint Scanning



some disadvantages, though. As the reader requires you to push your thumb or finger against a surface, it's easy to leave behind a latent print of the finger you just scanned. If some nefarious person were to find a good copy of your fingerprint on the surface, it wouldn't be impossible for them to make a copy of it and break into your computer. We'll explain how this could happen later.

SENSOR SENSIBILITIES

Aside from optical sensors, the most common method for scanning fingerprints is to use a capacitance sensor. Capacitance sensors rely on the principle of a capacitor; when you place two conductive plates close together, opposite charges can be stored on the two plates thanks to their mutual attraction. You can build a simple capacitor by placing two metal plates next to each other, with a gap between them, then connecting the two plates to the positive and negative terminals of a battery. The two plates become charged. With the battery removed, the energy previously stored in the plates is discharged.

Using two lengths of tin foil, separated by sheets of cling film and rolled up, you can build a reasonably effective capacitor that will hold enough energy for you to measure it with a multimeter when it discharges. Capacitors are used in lots of everyday electronic devices, but they can be dangerous. The large capacitors inside some hi-fi amplifiers and most CRT televisions can hold a significant charge. Capacitors are able to discharge rapidly, making them useful in devices such as electronic flashguns or amplifiers that need to drive large bass speakers. For the same reason, if you short-circuit a large capacitor by touching its terminals, it can give you a serious electric shock.

When they're not producing lethal jolts of electricity or helping car audio enthusiasts to disturb the neighbourhood, capacitors can also be used as a simple touch sensor. In a basic two-plate capacitor system, the amount of energy stored is affected by the distance between the two plates. Similarly, the charge stored is affected if a third, conductive item is

placed in the electrical field generated between the plates. This allows you to create a simple touch-sensitive switch by placing both plates of a capacitor under a thin layer of insulation. This capacitor will hold one charge when there is only air above the insulation, and a different level of charge when a finger above the insulation disturbs the field. By periodically measuring the charge held in the capacitor and waiting for it to change, a circuit can tell when a finger has been placed on the insulation to trigger the switch.

By building a grid of tiny capacitive switches under a rectangular area of insulation, you can use the information to ascertain which parts of the area are covered by a finger and which are not. By rapidly updating this information, it's possible to work out if the finger is being moved and in what direction.

This is how the touch pads found in most notebook computers work. Underneath the pad is an array of tiny capacitance sensors that detect your finger strokes and taps. By using smaller and more sensitive capacitance sensors, you can also read fingerprints. The ridges of a fingertip have a different effect on the capacitance of each sensor than the air present in the valleys between them. A simple capacitance fingerprint sensor uses a tiny but dense grid of these sensors to create a map of the ridges and valleys of any finger placed on it.

In real life, though, most capacitance fingerprint sensors don't use a square grid of sensors. Instead, they use a thin line of them. To use this kind of sensor, you swipe your fingertip across the sensor line. As you do so, it takes repeated measurements of the ridges and valleys on your fingertip. This kind of sensor has two distinct advantages over larger grid-based capacitance and optical sensors. It is smaller, making this kind of sensor easier to fit into notebook computers and other peripherals. Also, as the fingerprint is swiped rather than placed on the sensor, it does not leave behind a latent fingerprint that would be easy to copy.

SONAR, SO GOOD

Most commercial fingerprint scanners that you might attach to your computer or put in a door

lock use the optical or capacitive measurement techniques described above. There are alternative techniques, however. At least one manufacturer uses radio technology. Scanners such as the Biometrix 2600 series use radio waves to scan the surface of a finger from underneath. The sensor sends an RF wave up into the finger, where it reflects off the live fingertip skin just below the finger surface. An array of tiny antennas measures the reflected radio waves.

Just as a sonar system can detect the ridges and valleys of the sea bed by measuring the sound waves they reflect back through the water, this technology creates a map of the finger surface based on the pattern of radio waves reflected from the sub-surface live skin layer. The manufacturer of this technology, Authentec, claims that this technology allows a fingerprint to be taken even "if the valleys are worn away, filled with oil or dirt, or... smashed flat" and works with "even very dry skin". *Shopper* has no idea how one might go about getting their fingertips smashed flat, and nor do we particularly want to know.

MAN v SCANNER

There have been numerous examples of fingerprint sensors being tricked. Earlier this year the American TV programme *Mythbusters* tested to see how easily two fingerprint scanners could be fooled if one had access to a good-quality latent fingerprint from the authorised user. One, a fingerprint door lock, was beaten by simply producing an image of the fingerprint, printing it out from a computer, then sticking this black and white image on someone else's finger using saliva. It seems likely that this lock used an optical sensor, though no details were given.

The second sensor, attached to a computer via USB, was also fooled. To trick this second model, the hosts had to use a PCB etching kit to produce a 3D model of the fingerprint from a black and white image. This was used as a mould to produce a cast of the finger from ballistics gelatine, a substance designed to simulate human tissue. A Japanese researcher made headlines in 2002 using a similar method and household gelatine. Newer and more expensive devices may be more secure, but we'd always recommend securing any important data with a strong password and encryption software such as Steganos Security Suite 7.1.6, which is on this month's DVD.

FURTHER INFORMATION

www.bbc.co.uk/history/historic_figures/faulds_henry.shtml
Historical information on the founder of forensic fingerprinting

<https://webfiles.uci.edu/scole/MoreThan0.pdf>
Paper on the limitations of forensic fingerprint analysis

<http://www.freepatentsonline.com/4353056.pdf>
1982 Siemens patent for a capacitive fingerprint sensor

<http://www.schneier.com/crypto-gram-0205.html#5>
Defeating fingerprint readers with gelatine

www.zvetcobiometrics.com/Documents/Trueprinttechnology.ppt
Trueprint RF fingerprint technology